Title	PII Policy
Version	2
Effective Date	6/29/2020
Last Amended	6/29/2020
Department	Finance
Function	Information Technology (IT)
Policy Owner	Name: RC Woodson Title: BBNC VP of IT & CIO Direct Line: 907.265.7521 Email: rwoodson@bbnc.net

1. Purpose

Bristol Bay Native Corporation (BBNC) is committed to protecting your personal information. Personal Information can accumulate over time in a number of ways. The following Policy will assist all of us in understanding what that information is, how it can be protected and how we will work together to identify it and protect it. BBNC sets forth its protection of personally identifiable information (PII), in this PII Policy (Policy).

2. Overview

This Policy establishes how BBNC uses, stores, and destroys PII. It is the policy of BBNC to protect PII of its employees, customers, vendors and other third parties. The restrictions and safeguards outlined in this Policy provide guidance for the handling, storage and destruction of electronic and hard copy records that contain PII.

All employees are expected to read this Policy.

3. Scope

This Policy applies to BBNC Corporate. The Chief Information Officer (CIO) is responsible for ensuring this Policy is followed.

4. Definitions

Minimum Necessary means the least information and fewest people should be involved to satisfactorily perform a particular function.

Personally Identifiable Information (PII) means information that can be used to distinguish or trace an individual's identify.

PII includes the first name or first initial and last name of a person, in combination with one or more of the following data elements of the person:

- Social security number
- Driver's license number or state identification card number
- Passport or national identification number
- Tax identification number
- Financial account or payment card number and the means to access the account
- Biometrics used to authenticate the identity of the person
- Health insurance policy identification number
- Medical information identifying a physical or mental health condition
- Passwords, personal identification numbers, or other access codes that would permit access to financial or online accounts
- Government clearance forms containing one or more of the above data elements
- Educational transcripts in which the person is identified

PII does not include any information that cannot be associated with a particular individual, such as aggregate, anonymous or statistical data, or information that is publicly available.

5. Policy Statement

A. PROTECT YOUR PERSONAL INFORMATION (PII)

BBNC takes its responsibility to protect PII seriously. To prevent unauthorized access to or disclosure of PII, BBNC uses technical, physical, and administrative safeguards to protect PII and restrict access to PII by only those authorized employees or third parties with a legitimate business purpose to access the PII.

B. ACCEPTABLE USE

PII may only be received, processed, used, stored, transmitted, or disclosed for legitimate business purposes and in accordance with this Policy. PII may be released only on a minimum necessary basis and only to those individuals who are authorized to use such information as part of their official BBNC duties subject to the following:

- PII released is narrowly tailored to the specific business purpose(s)
- PII is kept secure and for the specific BBNC purpose for which authorization was obtained
- PII is not further disclosed or provided to others without proper authorization

Exceptions: BBNC may use or disclose PII in any one of the following limited circumstances that may not be directly associated with a legitimate business purpose:

- Emergencies for the benefit of the person from whom the PII was collected
- Protect the rights, property or safety of other persons
- Protect the rights or property of BBNC
- With the consent of the person from whom the PII was collected
- As permitted or required by applicable law or legal process
- To law enforcement or other civil parties when, in the opinion of BBNC, such disclosure is necessary to prevent fraud or to comply with any statute, law, rule or regulation of any governmental authority or any order of any court of competent jurisdiction
- When such information is otherwise publicly available

C. RESTRICTIONS ON THIRD-PARTY ACCESS TO AND USE OF PII

BBNC will impose controls and contractual obligations on approved third parties to whom BBNC may disclose PII for legitimate business purposes. Approved third parties will be contractually obligated to maintain the confidentiality and security of PII. They will be restricted from using, transmitting or disclosing PII in any way other than to render legitimate business services to BBNC. BBNC may conduct audits to ensure compliance with this Policy and applicable laws.

D. DATA RETENTION AND DESTRUCTION

Unless subject to a Legal Hold Notice or other extenuating circumstances, BBNC will retain collected PII only so long as there is a legitimate business purpose for its retention, or as permitted or required by law. BBNC will dispose of collected PII when there is no longer a legitimate business purpose for its retention, or retention is no longer permitted or required by law. PII must be disposed of in a way that renders the information unreadable, indecipherable, unable to be reconstructed, or unable to be traced to a particular individual.

E. METHODS TO PROTECT AND SECURE PII

To the extent that PII is received, processed, used, stored, or disclosed, the following technical, physical, and administrative methods are required to protect and secure PII

under BBNC's control. These measures are applicable to PII store both on and off BBNC property:

- Electronic and physical access to PII must be limited to those authorized employees and third parties who have a legitimate business purpose to access the PII
- Authorized employees or third parties may not electronically transmit PII unless it is encrypted, password protected, or otherwise secured
- PII may not be sent wirelessly or over a public network unless the data or transmission path is encrypted
- PII at rest must be encrypted
- PII on mobile devices and mobile computing platforms (e.g., smartphones, tablets, E-readers, and notebook computers) must be encrypted
- PII must be physically protected from inadvertent or unauthorized disclosures, and authorized users must keep PII from the view of unauthorized users
- Physical media containing PII – including hard drives, servers, and portable media – must only be physically accessible to authorized users with unique user identifications and passwords, and it must otherwise be securely stored
- Electronic access to PII must be restricted to active, authorized users with unique user identifications and passwords

F. RISK ASSESSMENT

BBNC will periodically assess risks to operations (including mission, functions, image, or reputation), assets, and individuals resulting from the operation of information systems and the associated processing, storage, and/or transmission of PII.

6. Related Policies, Procedures, and Guidelines

Cloud Computing Policy
Data Access and Protection Policy
Data Categories Policy
Data Privacy and Security Policy
Vendor Management Policy

7. Supporting Documents and Additional Information

Data Categories Visual Aid

8. Storage

This Policy can be found on One Drive and on the InfoNet Policy Library.